

JapanTechnicalJamboree69

OpenChain仕様の活用を視野に入れた SW360運用について

How to use SW360 aimed at observing OpenChain specification.

TOSHIBA

株式会社 東芝 研究開発本部

ソフトウェア技術センター

オープンソース技術部 浜 功樹

kouki1.hama@toshiba.co.jp

2019.05.24

© 2019 Toshiba Corporation

Contents

01 前回発表の振り返り「SW360とは？」

02 SW360とOpenChainの仕様

03 SW360とTooling SubWG

04 まとめ

Contents

01 Preview 「What is SW360 ? 」

02 SW360 and OpenChain Specification

03 SW360 and OpenChain Japan Tooling SWG

04 Conclusion

01

前回の振り返り「SW360とは？」

01

Preview 「What is SW360 ? 」

SW360とSW360のインストール方法

- 前回の発表
 - <https://elinux.org/images/3/31/SW360-JapanTechnicalJamboree67-2.pdf>
- インストール方法紹介
 - OSS管理ツール SW360 - オープンソースをオープンソースで管理しよう
 - <https://qiita.com/K-Hama/items/90a6105a16400ce3e718>
- 設定方法
 - OSS管理ツール SW360 - オープンソースをオープンソースで管理しよう（2. 設定編 その1）
 - <https://qiita.com/K-Hama/items/c66d9becf9aeb8f8863e>
- Github
 - <https://github.com/eclipse/sw360>
- メーリングリスト
 - <https://accounts.eclipse.org/mailling-list/sw360-dev>
 - <https://accounts.eclipse.org/mailling-list/sw360-users>

What is SW360? And How to Install SW360

- Previous Presentation
 - <https://elinux.org/images/3/31/SW360-JapanTechnicalJamboree67-2.pdf>
- How to install (Japanese)
 - OSS管理ツール SW360 - オープンソースをオープンソースで管理しよう
 - <https://qiita.com/K-Hama/items/90a6105a16400ce3e718>
- How to set (Japanese)
 - OSS管理ツール SW360 - オープンソースをオープンソースで管理しよう （2. 設定編 その1）
 - <https://qiita.com/K-Hama/items/c66d9becf9aeb8f8863e>
- Github
 - <https://github.com/eclipse/sw360>
- Mailing list
 - <https://accounts.eclipse.org/mailling-list/sw360-dev>
 - <https://accounts.eclipse.org/mailling-list/sw360-users>

02

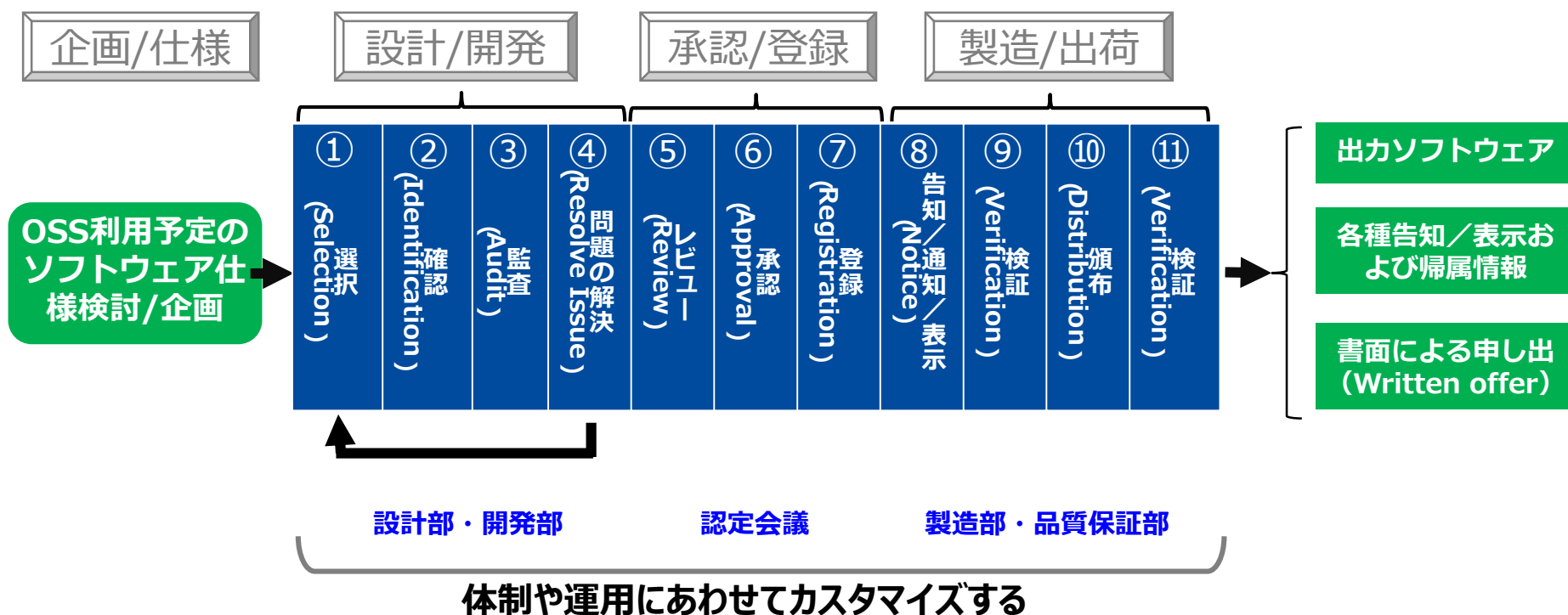
SW360とOpenChainの仕様

02

SW360 and OpenChain Specification

OSSを利用するためのプロセス

Open Chain プロセスに準拠



1.2 準拠

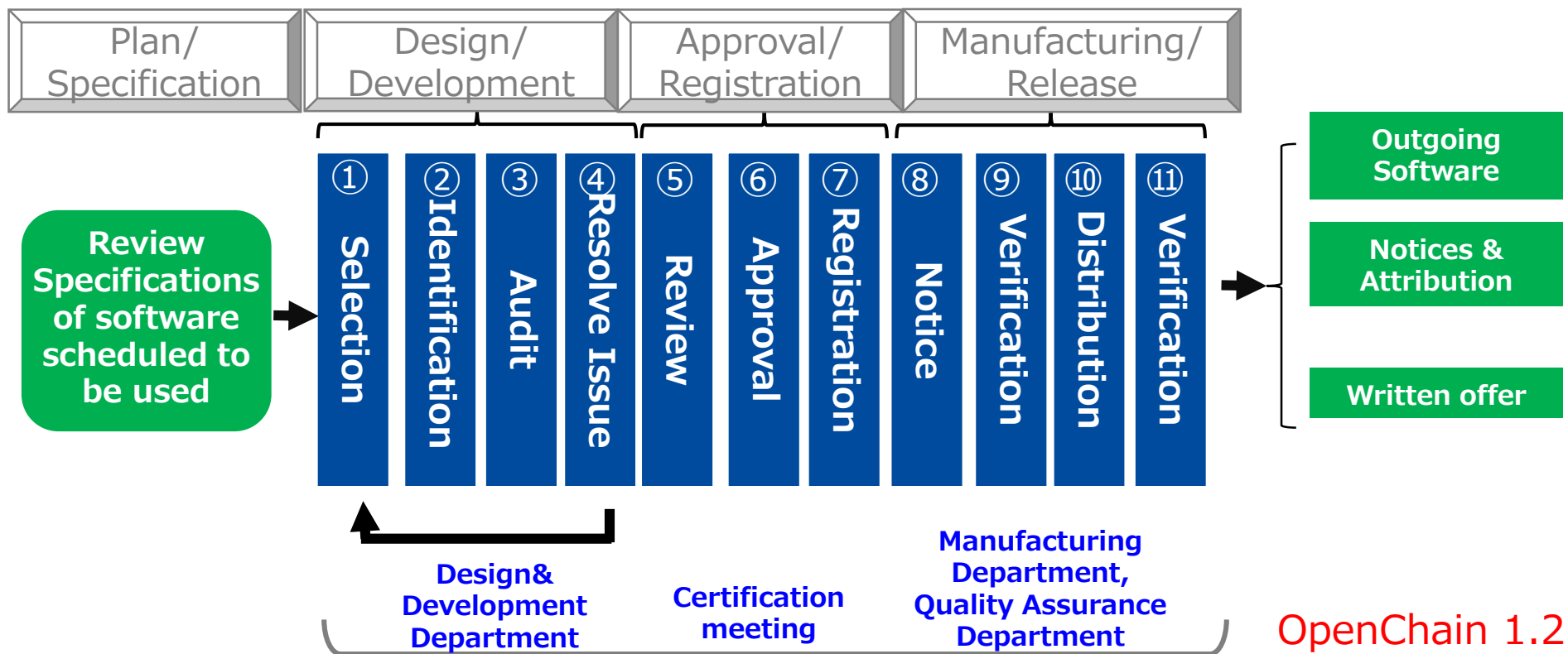
参考: <https://www.openchain.org>

<https://www.slideshare.net/ShaneCoughlan3/giving-everyone-access-to-open-source-best-practices-the-openchain-curriculum>

備考: ステップ①選択を追加

Example OSS Using Process

Apply for Open Chain Processing



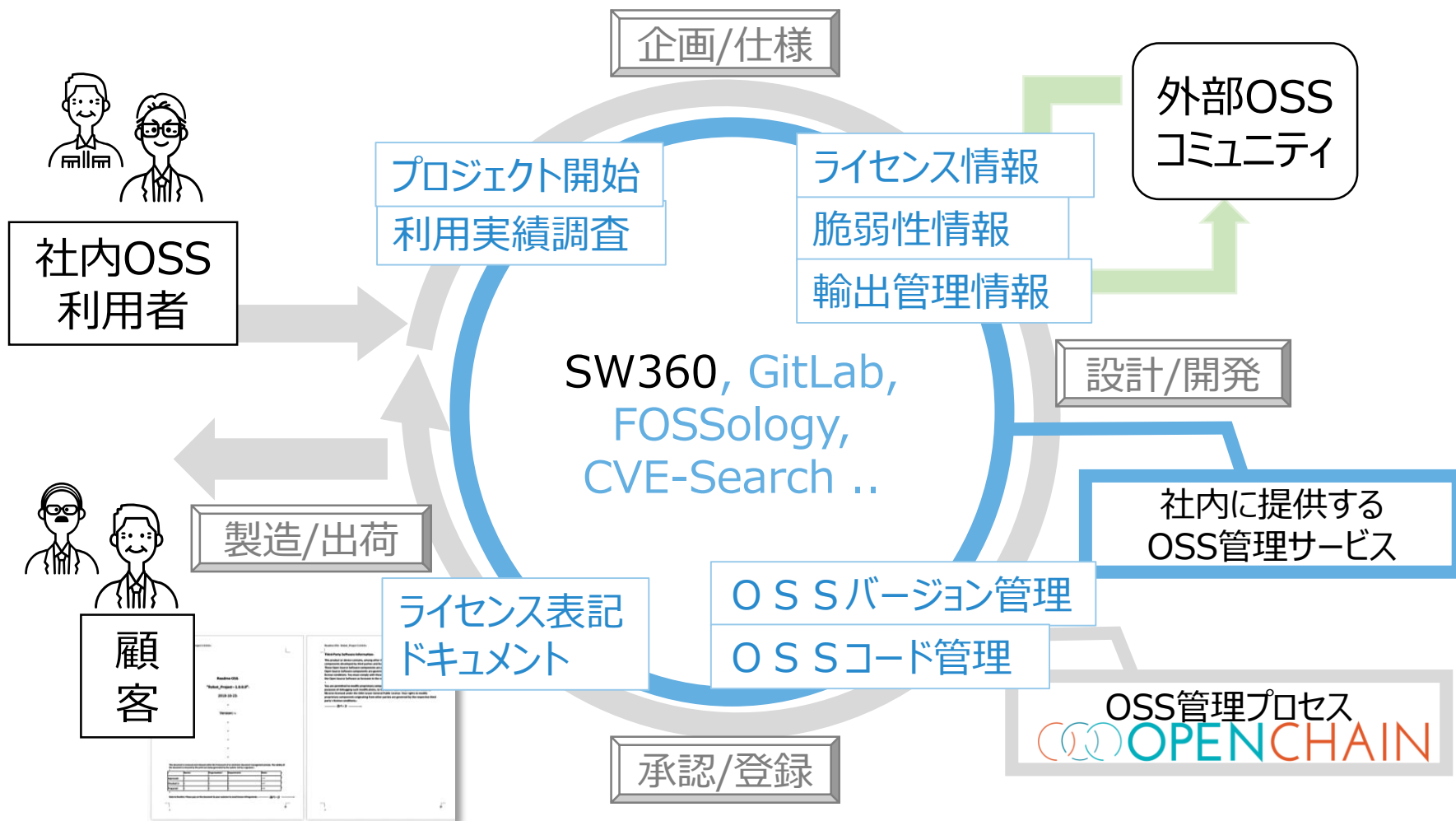
Example of Compliance Management End-to-End Process

Ref: <https://www.openchain.org>

<https://www.slideshare.net/ShaneCoughlan3/giving-everyone-access-to-open-source-best-practices-the-openchain-curriculum>

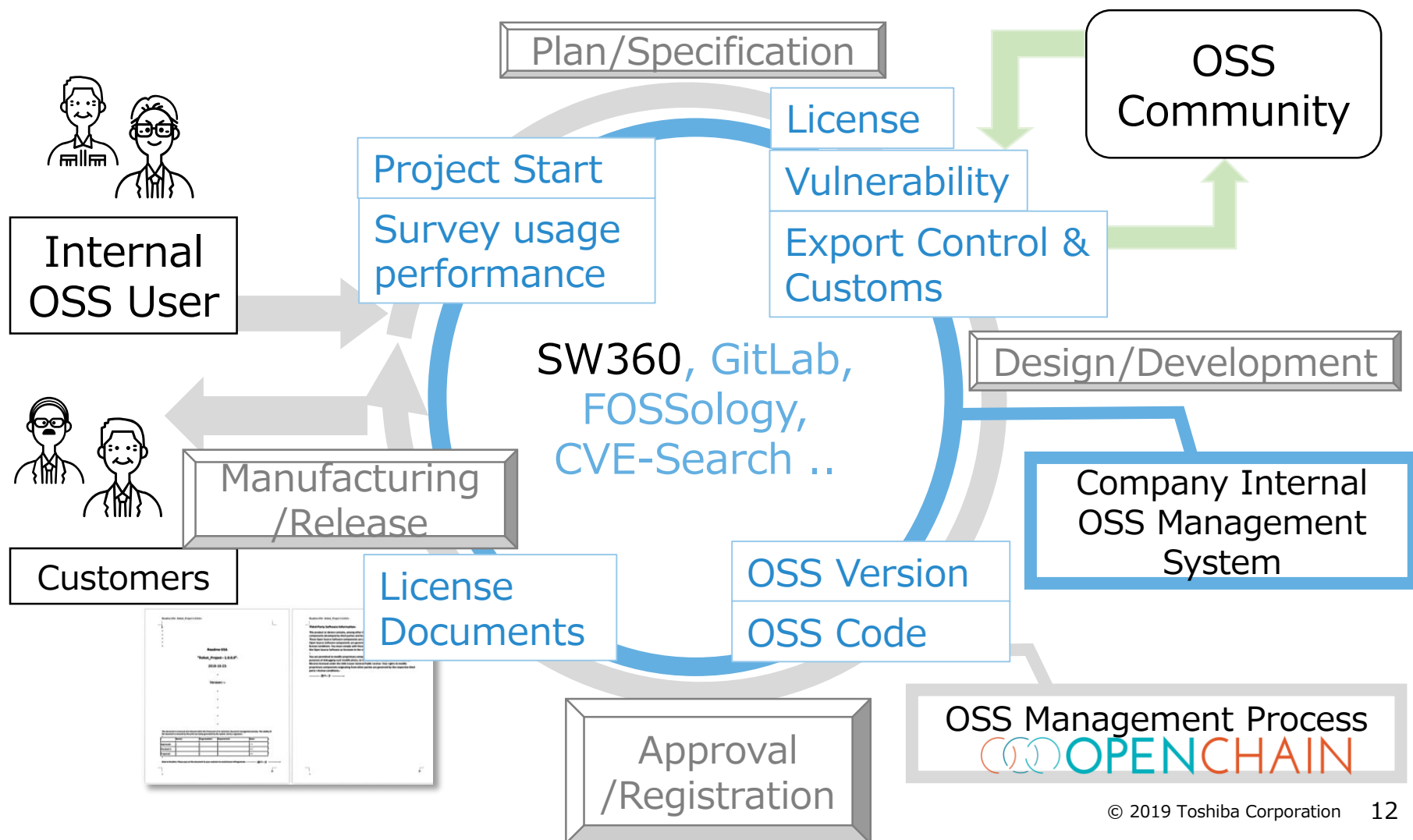
Note: Add step ① Selection

OSS活用・管理プロセスと一体運用（概案）



OSS Management and SW360

Using and Managing OSS system (Concept)



OSS情報のバージョン管理システム

プロジェクト情報とOSSコンポーネントを紐付けて管理する

プロジェクト管理画面

General

Name *
Enter Name

Version
Enter Version

Project visibility *
Group and Moderators

Created by
Will be set automatically

Home Page URL
Enter Home URL

Wiki URL
Enter Wiki URL

Project type *
Customer Project

Tag
Enter one word tag

Description
Enter Description

Enable Security Vulnerability Monitoring

Enable Displaying Vulnerabilities

Roles

Group *
Toshiba

Project manager
Click to edit

Project owner
Click to edit

Owner accounting unit
Enter owner's accounting unit

Owner billing group
Enter owner's billing group

Lead architect
Click to edit

Security Responsibilities
Click to edit

Additional Roles

Click to add row to Additional Roles

External ids

Click to add row to External ids

プロジェクト名、バージョン、
開示範囲、開発タイプ、
開発部門、開発リーダ、等

OSSごとのコンポーネント管理画面

Edit

Delete libjavascrip-common (0.0.0)

Release Summary

Vendor
Click to set vendor

Name *
libjavascrip-common

Version *
0.0.0

Programming Languages
e.g., Java, C++, C#, ...

Operating Systems
e.g., Linux, MAC, Windows, ...

CPE ID
cpe:2.3:-:apache:traven:1

Release Date
2018-09-21

Licenses
GPL-2.0+

Download URL
Enter URL

Cleaning State
New

Release Maritime State
Maritime

Created by
Kobu Hama

Contributors
Click to edit

Moderators
Click to edit

Additional Roles

Click to add row to Additional Roles

External ids

Click to add row to External ids

Release Repository

Repository Type
Unknown

OSS名、ベンダ、バージョン、
言語、OS、著作者、入手元、
ライセンス、脆弱性検索キー、等

相互に関連付けられる

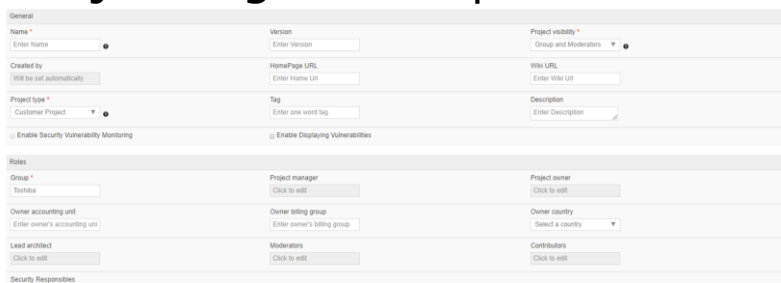
OSS情報

Management information by SW360

Management OSS component version

Management and Associate Project Information With OSS Component

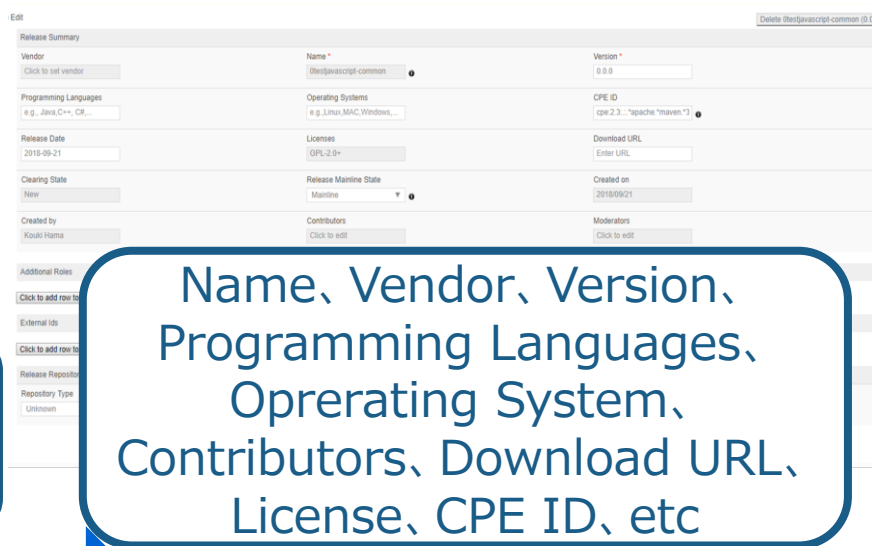
Project register snapshot



A screenshot of the 'Project register' form in SW360. It is divided into two main sections: 'General' and 'Roles'. The 'General' section includes fields for Name, Version, Project visibility, Created by, HomePage URL, Wiki URL, Project type, Tag, Description, and checkboxes for 'Enable Security Vulnerability Monitoring' and 'Enable Displaying Vulnerabilities'. The 'Roles' section includes fields for Group, Project manager, Project owner, Owner accounting unit, Owner billing group, Owner country, Lead architect, Moderators, and Contributors, each with a 'Click to edit' button.

Name, Version,
Project visibility, Project type,
Group, Project owner, 等
Group, Project owner, 等

Component register snapshot



A screenshot of the 'Component register' form in SW360. It is divided into two main sections: 'Release Summary' and 'Additional Roles'. The 'Release Summary' section includes fields for Vendor, Name, Version, Programming Languages, Operating Systems, CPE ID, Release Date, License, Download URL, Clearing State, Release Maritime State, Created by, Contributors, and Moderators. The 'Additional Roles' section includes fields for External ids, Repository Type, and Repository URL. A blue box highlights the following fields: Name, Vendor, Version, Programming Languages, Operating System, Contributors, Download URL, License, CPE ID, etc.

Name, Vendor, Version,
Programming Languages,
Opererating System,
Contributors, Download URL,
License, CPE ID, etc

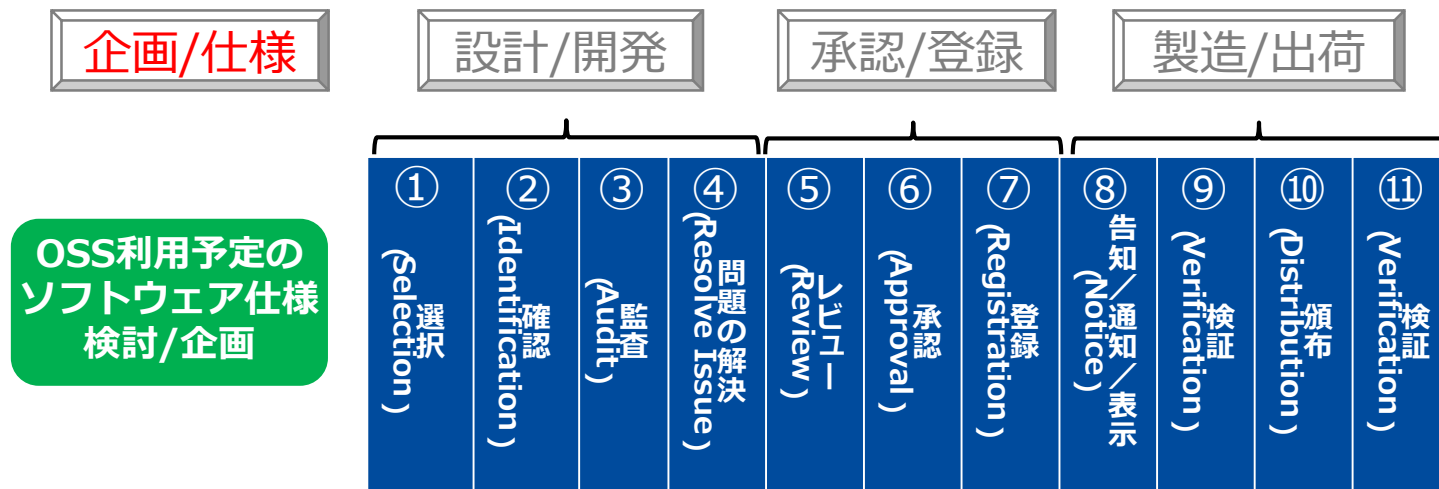
OSS Information

Linked each other

OSS利用時の導入

SW360:

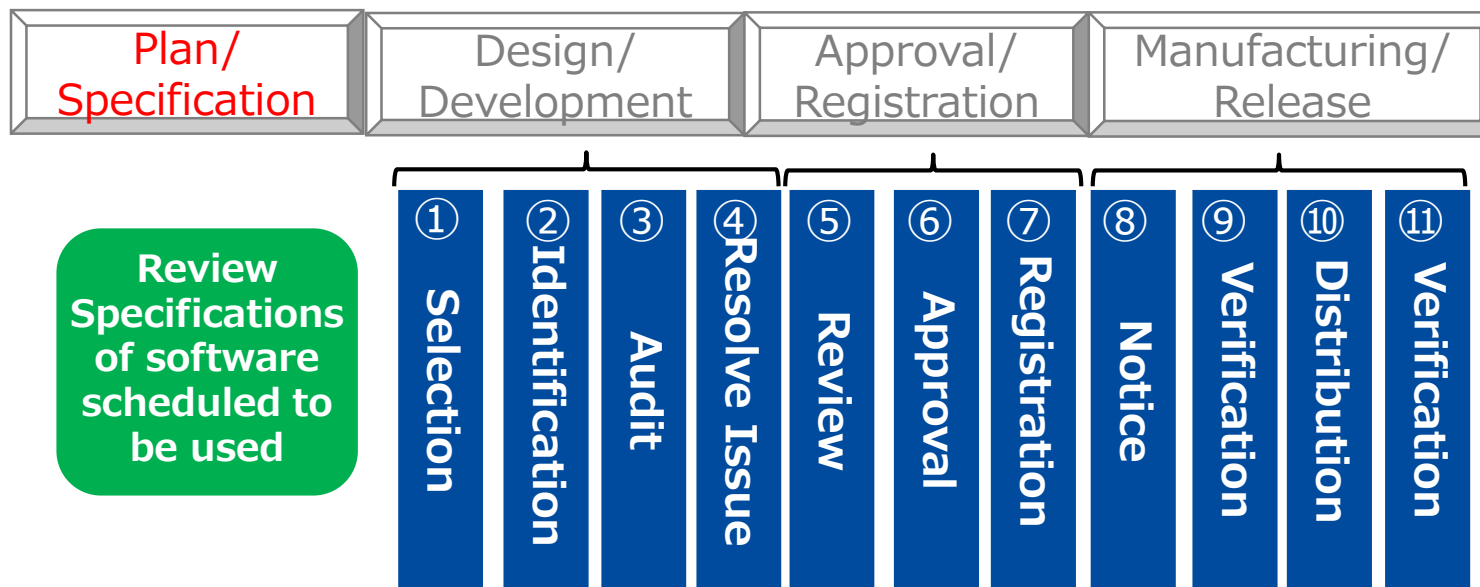
- ❑ 該当するプロジェクトを作成する
- ❑ 既存のプロジェクトがある場合は、適切であることを確認する
- ❑ プロジェクトに携わるメンバを決め、プロジェクトに対するアクセス権限を設定する



Beginning of using OSS

SW360:

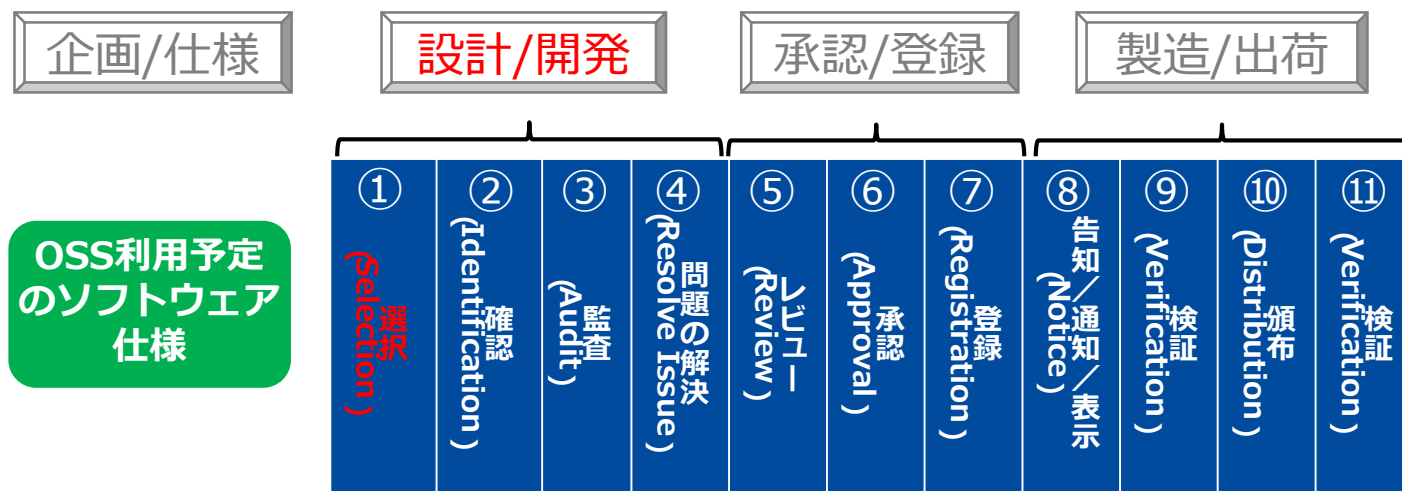
- ❑ Create new project
- ❑ If an existing project exists, make sure that it is appropriate
- ❑ Determine the project participants and give them appropriate access right



① 選択

SW360 :

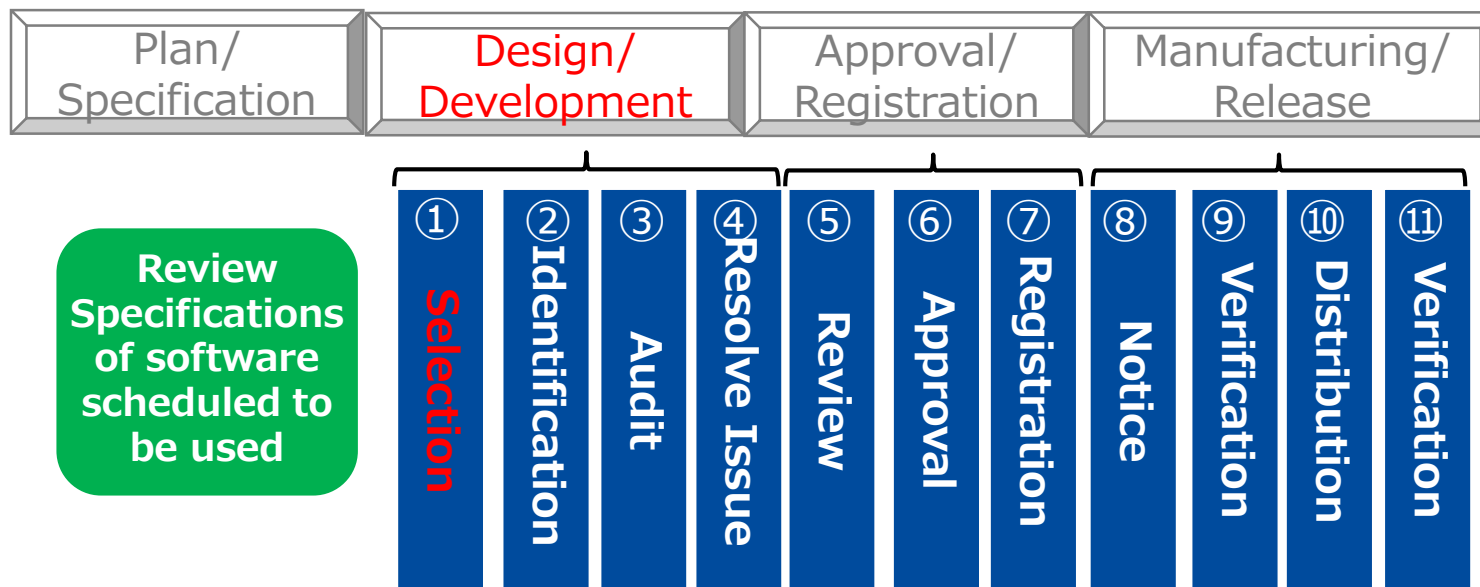
- 使用予定のコンポーネント(OSS,商用ソフト等)をリストアップ
- 必要に応じて過去の使用実績などを参照する



① Selection

SW360 :

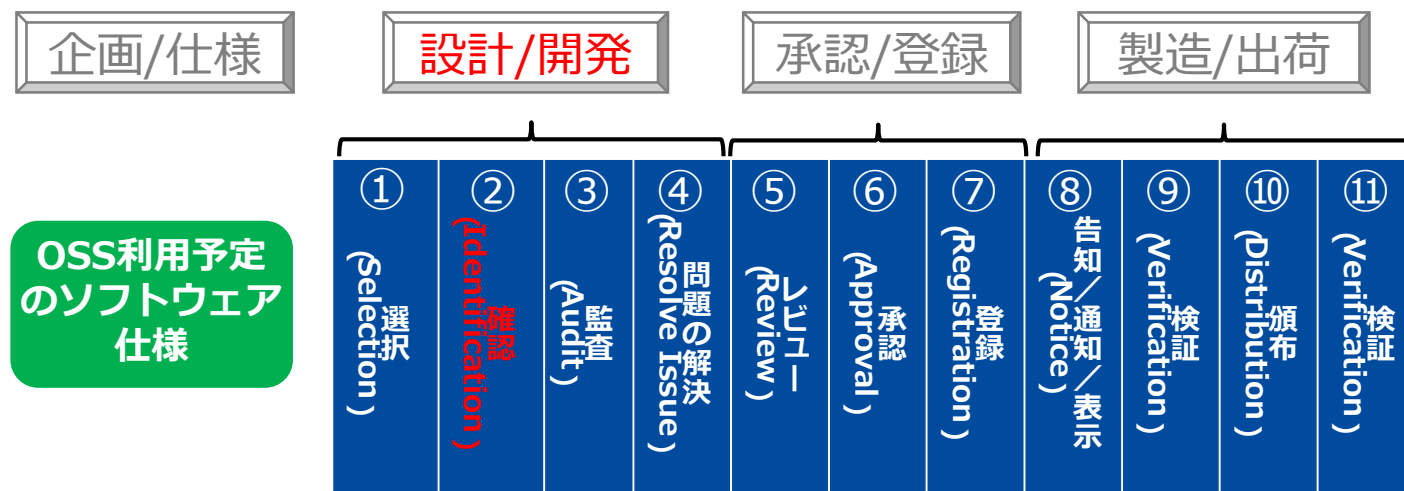
- ❑ Confirmation of used components
(ex. OSS, commercial software, etc.)
- ❑ If necessary, refer to past usage records etc.



② 確認

SW360 :

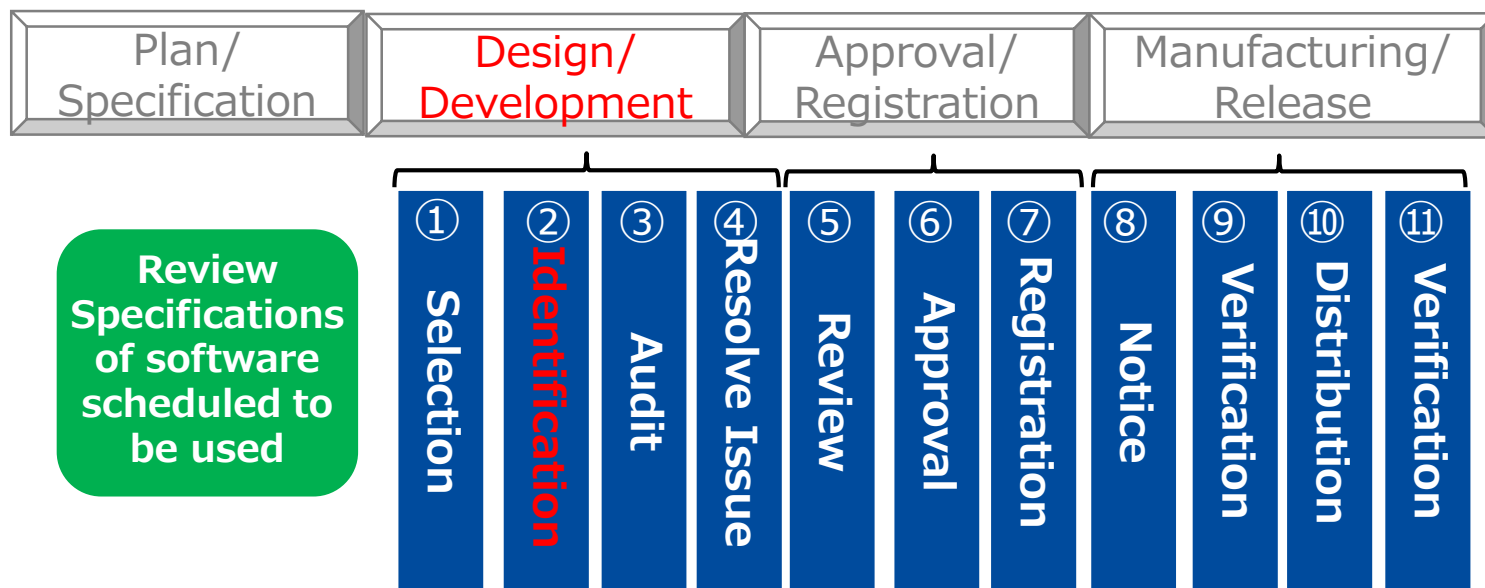
- 使用コンポーネント(OSS)情報(名称、バージョン、入手元、その他入力可能な情報)を登録する
- OSS入手元のソースコードを確認する
- OSSを使用する開発に利用することを登録
- OSS管理責任者が承認



② Identification

SW360 :

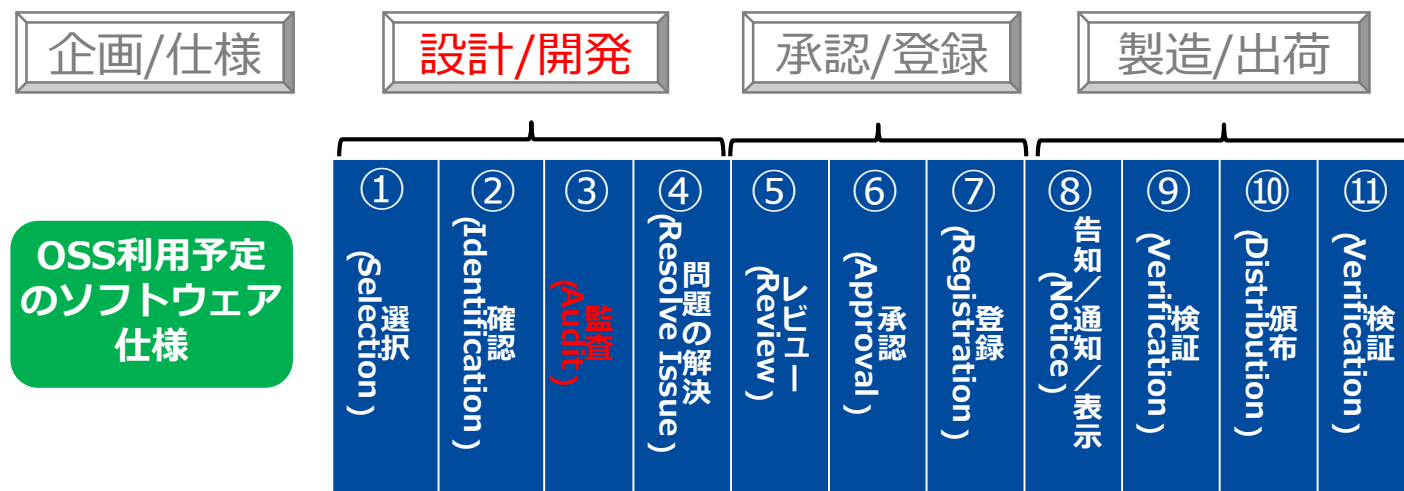
- ❑ Register used component (OSS) information (name, version, acquisition source, and other information that can be entered)
- ❑ Check the source code of OSS source
- ❑ Register to use OSS
- ❑ OSS administrator approves



③ 監査

SW360(要検討)：

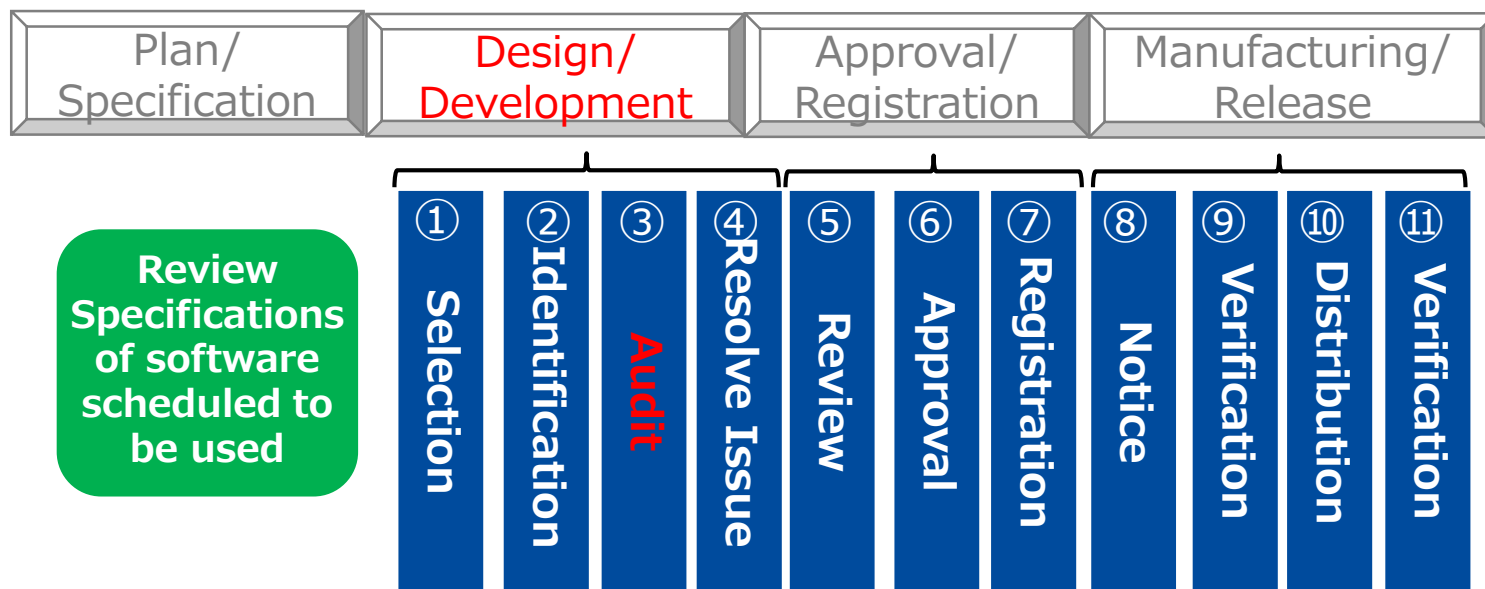
- OSSソースコードを登録 (バージョン管理)
- ライセンススキャン (ライセンス情報取得/Fossology)
- コードスキャン (未知のOSS検出)
- OSS使用状況を登録 (設計仕様管理)
- コンポーネント脆弱性検索キー(CPE ID)を設定
- コンポーネント輸出管理関連情報を設定



③ Audit

SW360(To Be Discussed) :

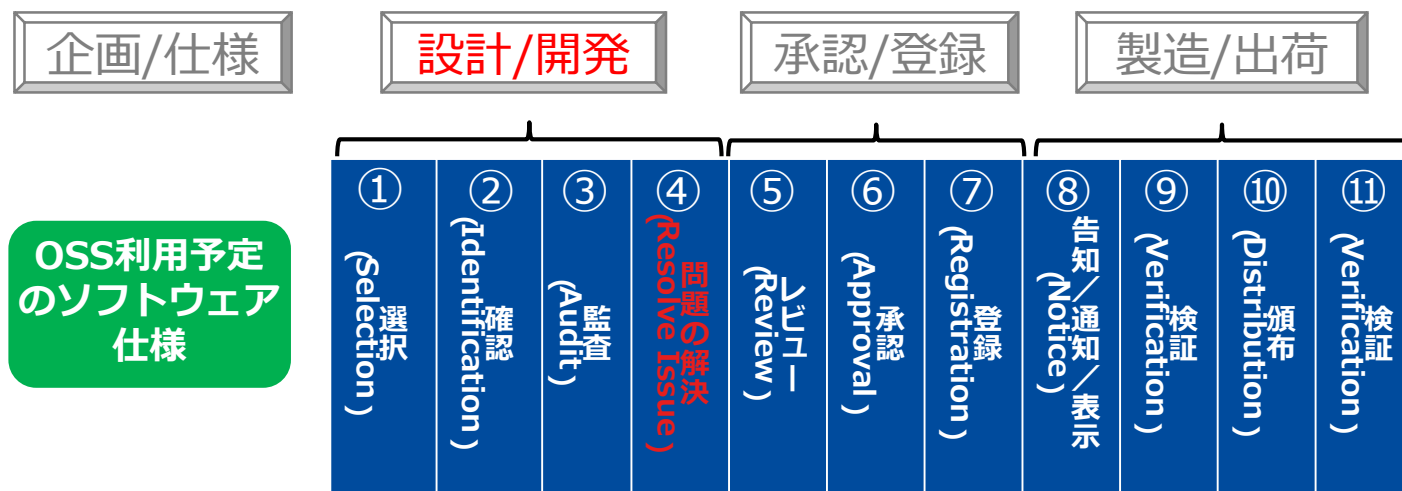
- ❑ Register OSS Source code (with version)
- ❑ License scan (License information from Fossology)
- ❑ Code Scan (For detection unknown OSS)
- ❑ Register OSS Usages (For design specification / management)
- ❑ Register CPE ID (For detecting vulnerability)
- ❑ Register ECC (Export Control) Information



④ 問題の解決

SW360 :

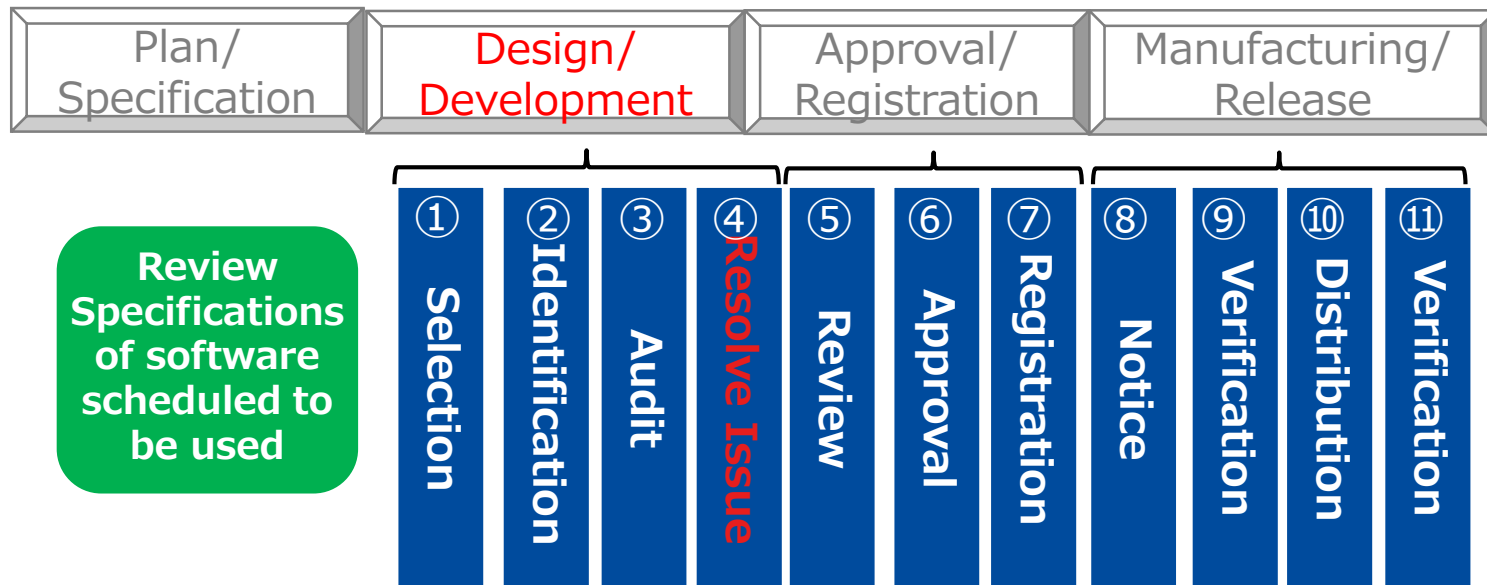
- コンポーネント登録情報の更新
- 構成管理表 (BoM) 出力 (レビュー用情報)



④ Resolve Issue

SW360 :

- ❑ Update Component Information
- ❑ Bill of Material document output (For review)



⑤ レビュー

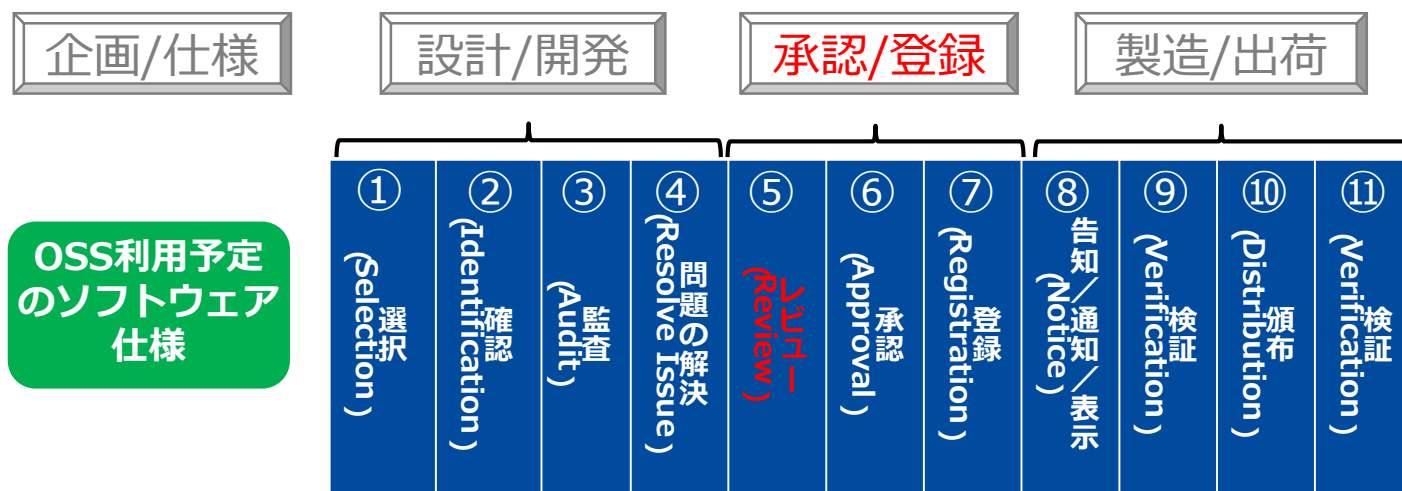
SW360 :

□レビュー実施記録

例えば以下のレビュー結果を保存

- ・ OSSライセンスの問題の解決が完了していることを検証
- ・ アーキテクチャ・レビュー : OSSと自製コードの構造検証
- ・ リンク解析レビュー : LGPLのリンク方法について検証

→ 問題が見つかった場合は開発部門へ対応を依頼



⑤ Review

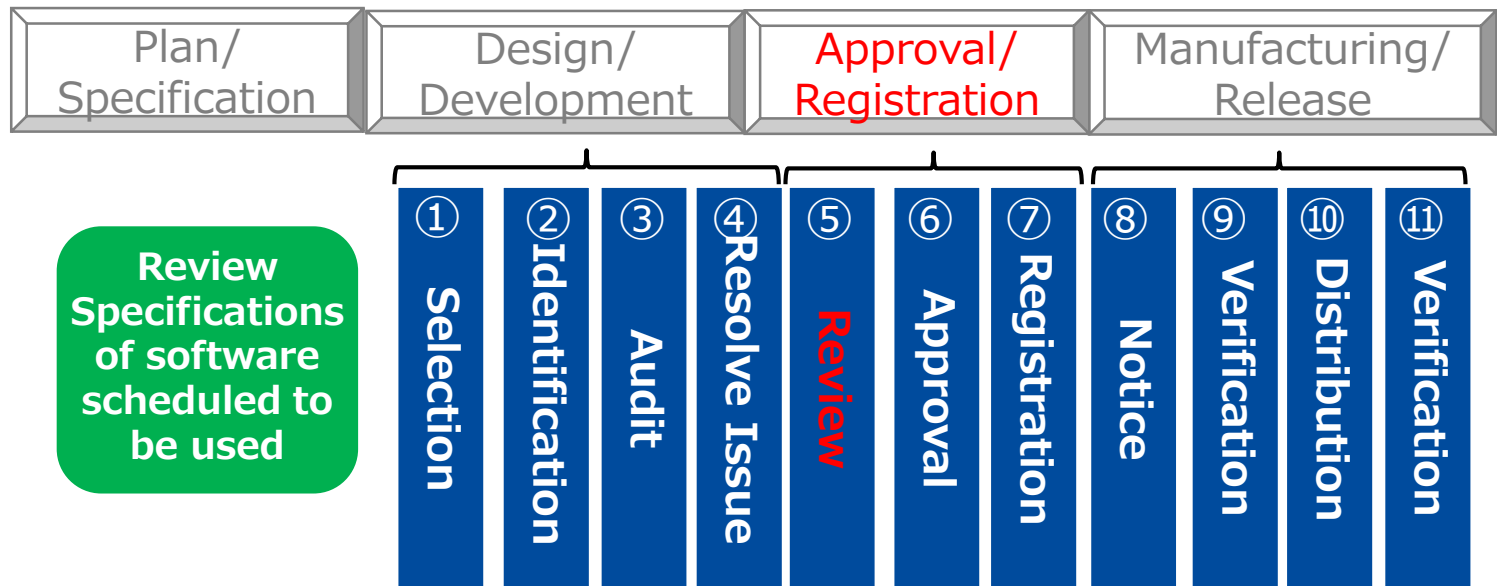
SW360(To Be Discussed) :

❑ Register implementation record

Example:

- Finish solve all license conflict issues?
- Architecture review : OSS and Self-made source code
- Link Review : Especially, connect with LGPL source code

→ If you find any kinds of problem,
you need to report develop department.



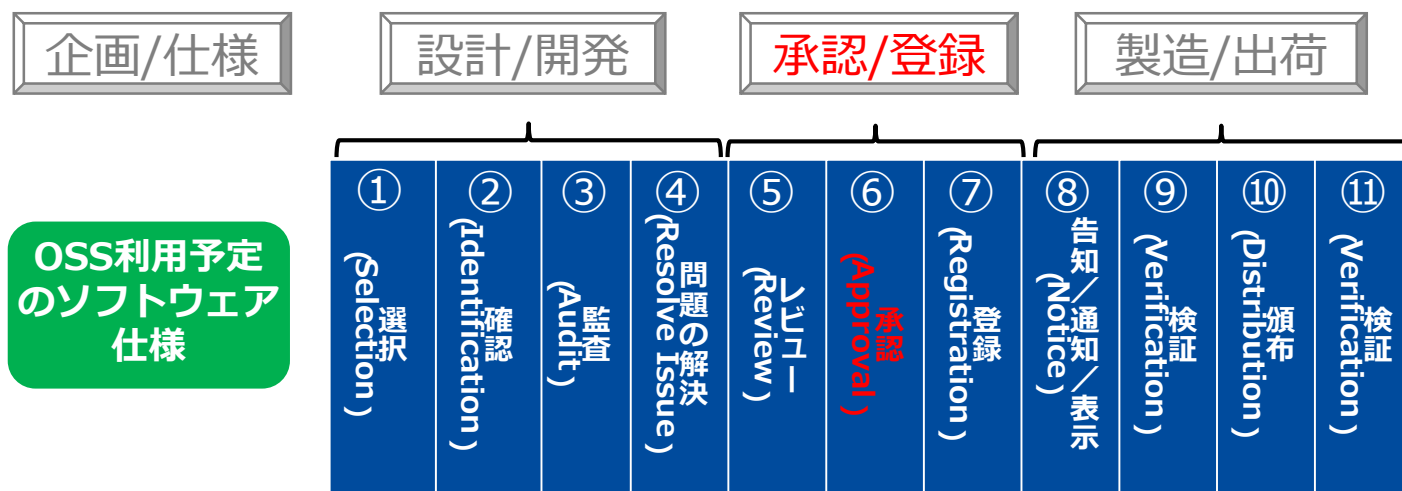
⑥ 承認

SW360(要検討)：

□承認（承認者、日時、付帯条件、等）を記録

ここでやりたいこと

- ・OSS使用に関する全ての確認、レビューが完了していることを検証する
- ・承認する場合は、製品部へOSS使用条件を伝達する
- ・否認する場合は、開発担当へ理由を明らかにする



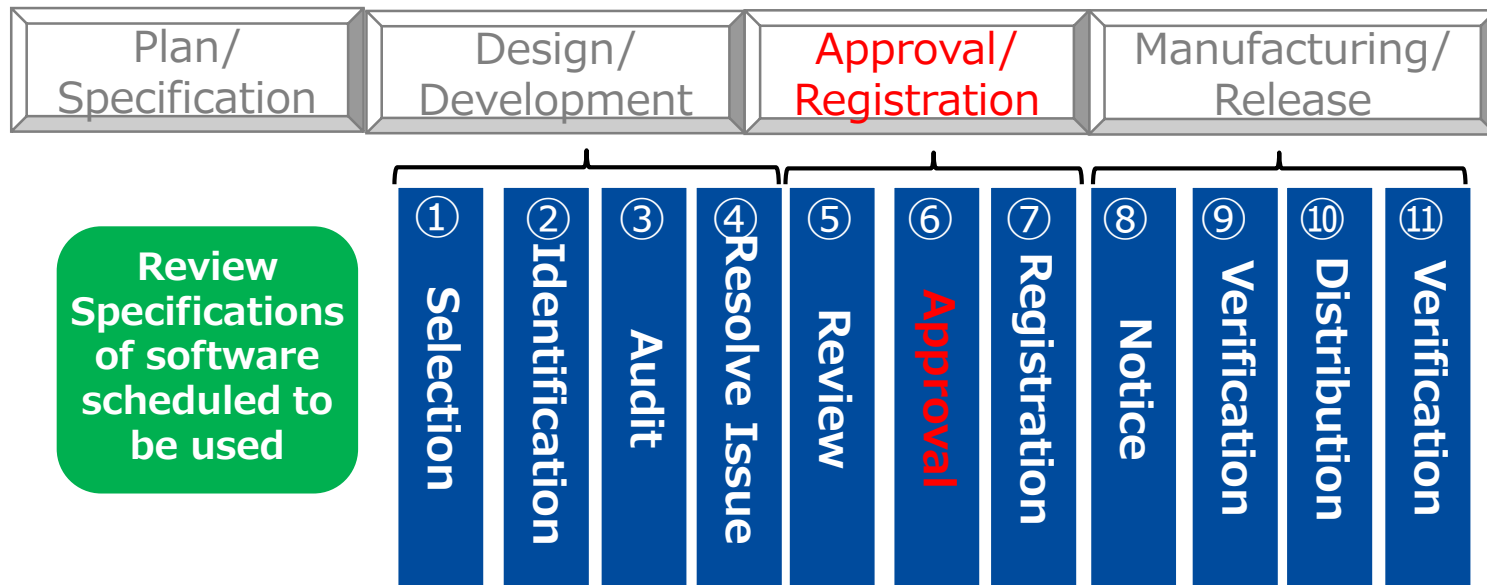
⑥ Approval

SW360(To Be Discussed) :

- ▣ Record Approval Information
(Approver, Date, Incidental condition, etc.)

This step's goal

- Verify that all confirmations and reviews of OSS usage have been completed
- Approve : Announced the OSS conditions of use to the Manufacturing department
- Disapprove: Announced the reason for manufacturing department

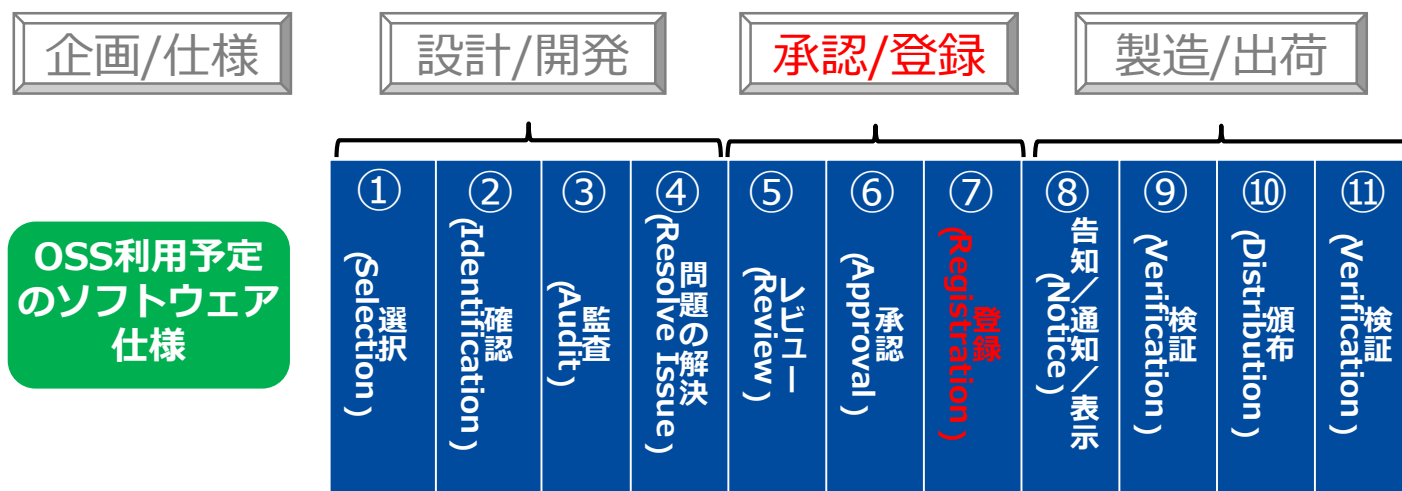


⑦ 登録

SW360(要検討)：

□OSS名、バージョン、社内担当者、使用するプロジェクト、プロジェクトのバージョン、など詳細を記録する

備考:現在 登録ルール/詳細検討中

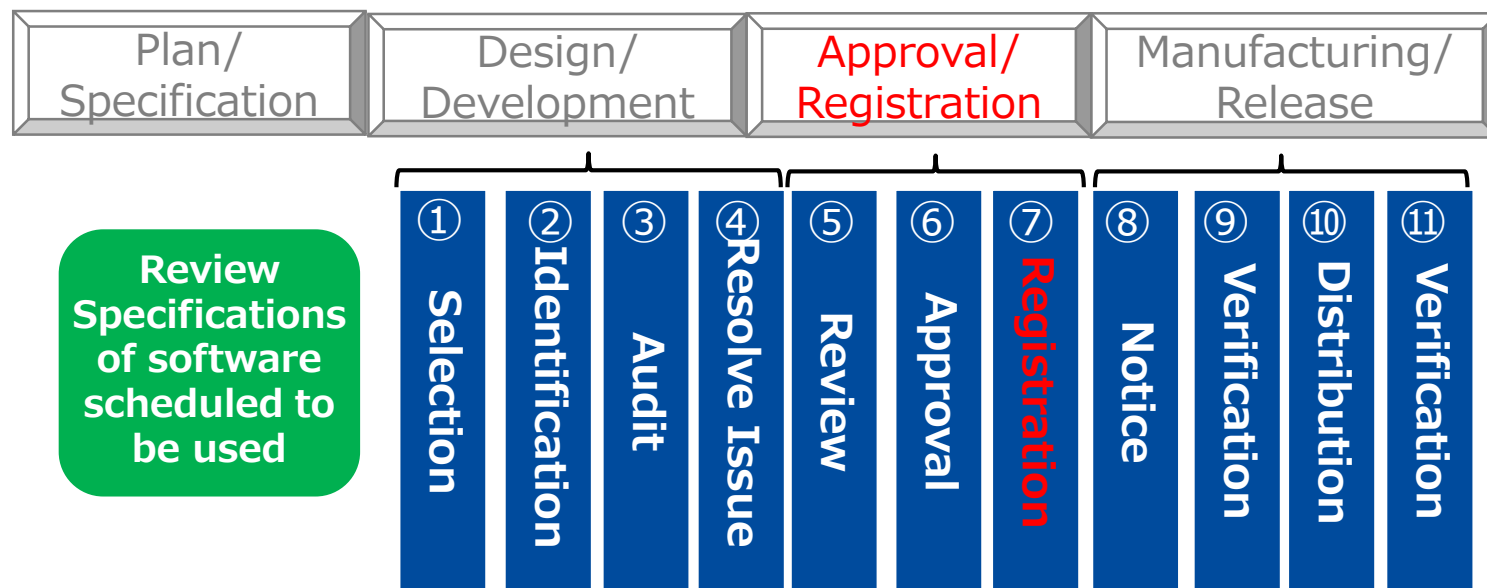


⑦ Registration

SW360(To be discussed) :

□OSS (Name, Version, Person in charge, etc.)
And Projects (Name, Project Version, etc.)

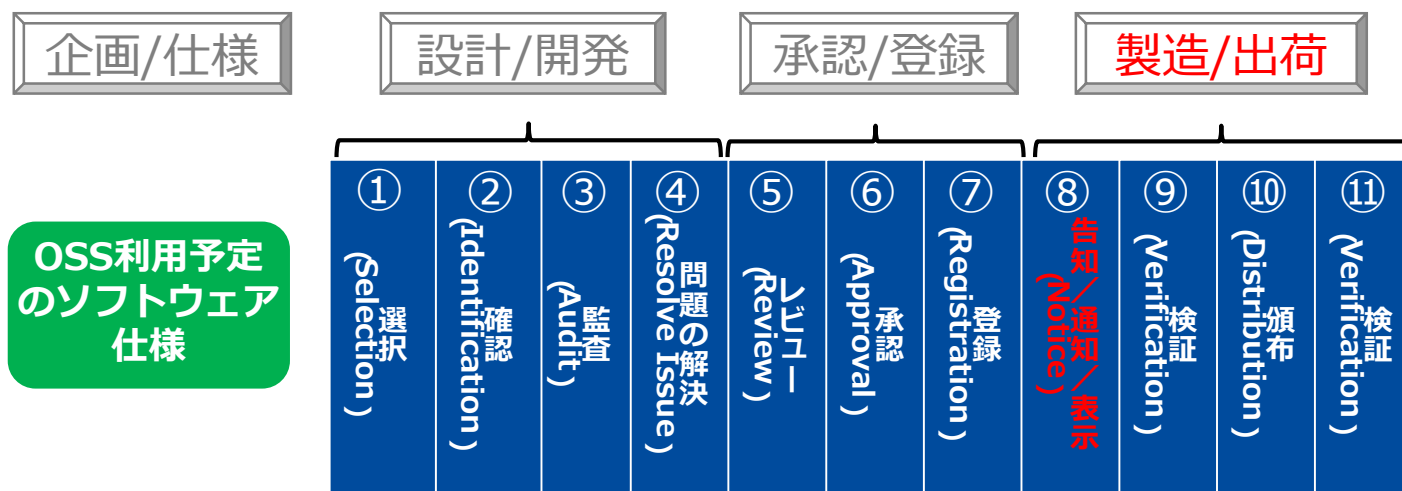
Note : Need operational rules?



⑧ 告知／通知／表示

SW360 :

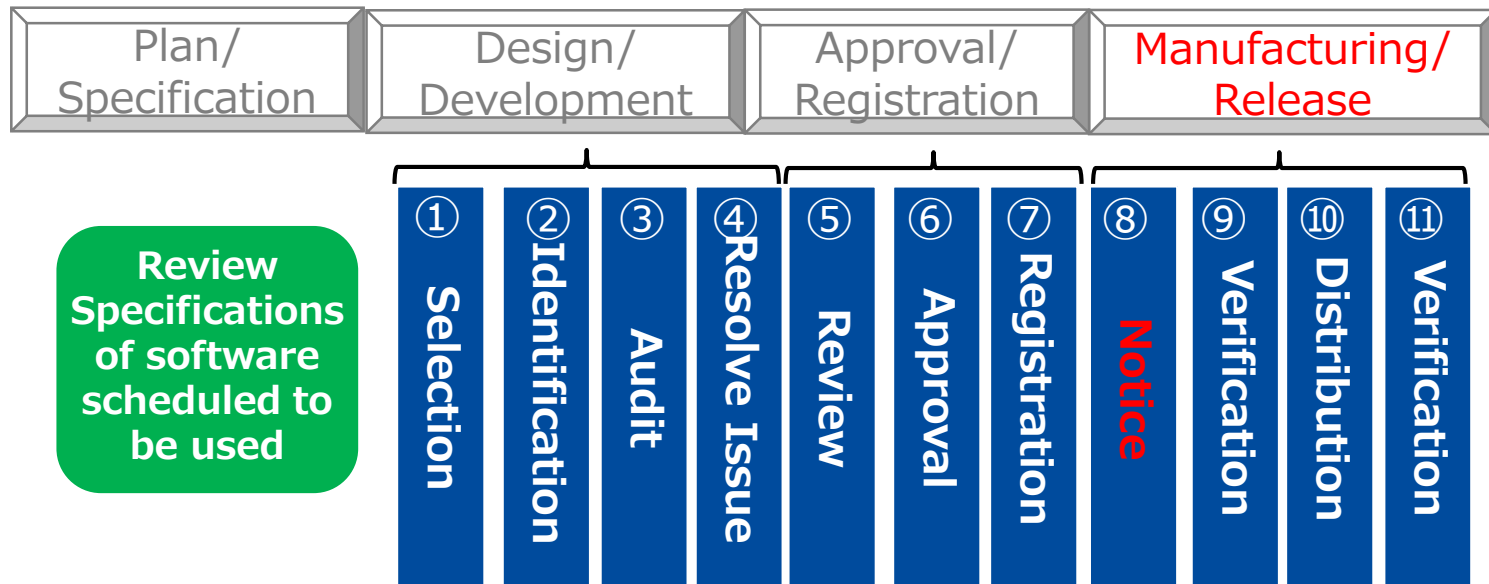
- 著作権リスト、ライセンスリストを成型する
- 製品添付文書のフォーマットを登録、文書出力する



⑧ Notice

SW360 :

- ❑ Create easy-to-read copyright and license list
- ❑ Register the format of the product attachment and output the document



⑨ 出荷前検証

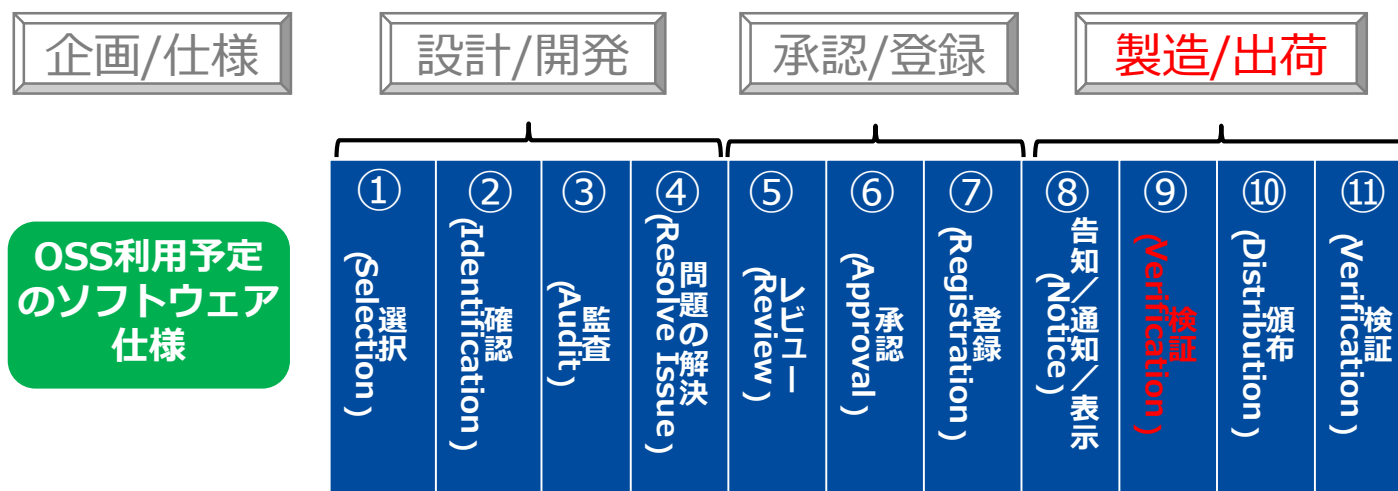
SW360(要検討)：

❑登録情報が正しいことを最終確認

❑告知文書等が登録されることを確認

- ・ OSSを含むコードの配布方法を決定/選択する
- ・ 配布用ソースコードと製品バイナリの一致を確認する
- ・ 告知文書がライセンスを満たすことを確認する
- ・ 公開用ソースコードに余分な情報が無いようにする(コメント文など)

→ 実施状況・ワークフローを確認できるようにする

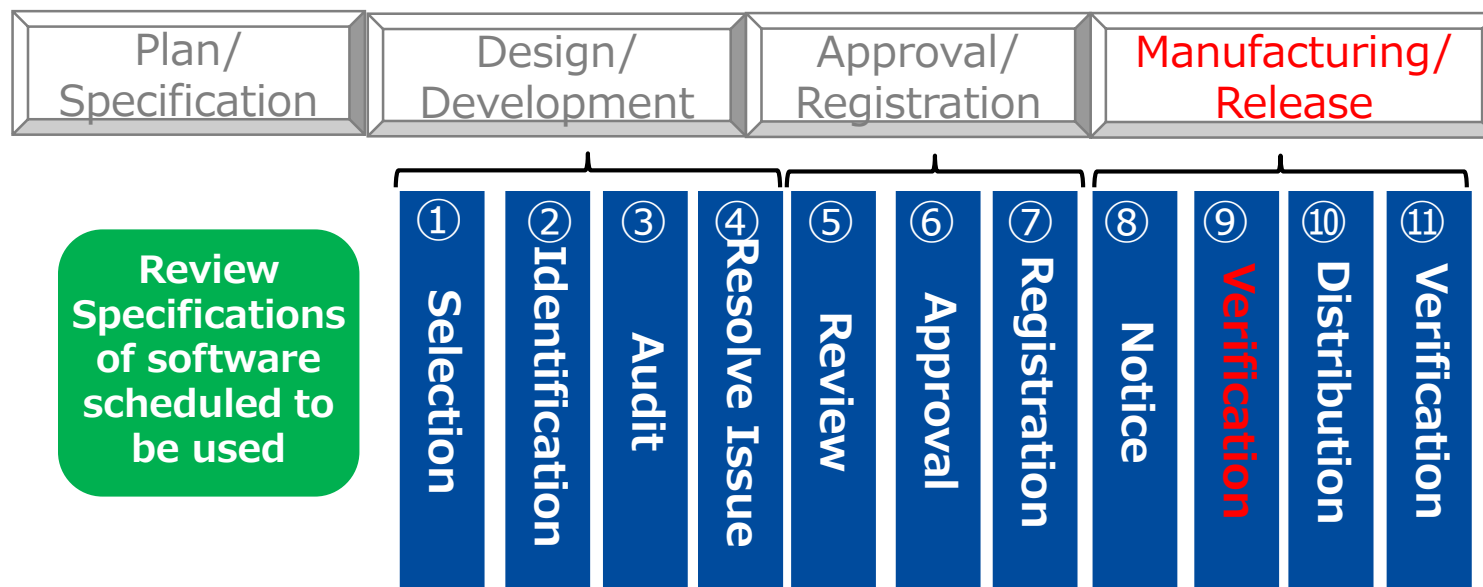


⑨ Verification

SW360(To be discussed) :

- ❑ Final confirmation that registration information is correct
- ❑ Confirm that notice documents etc. are registered
 - Determine how to distribute code that includes OSS
 - Confirm that the distribution source code matches the product binary
 - Confirm that the notice document meets the license
 - Make sure there is no useless information (such as useless comments) in the public source code

→ Need to make it possible to check the implementation status and workflow



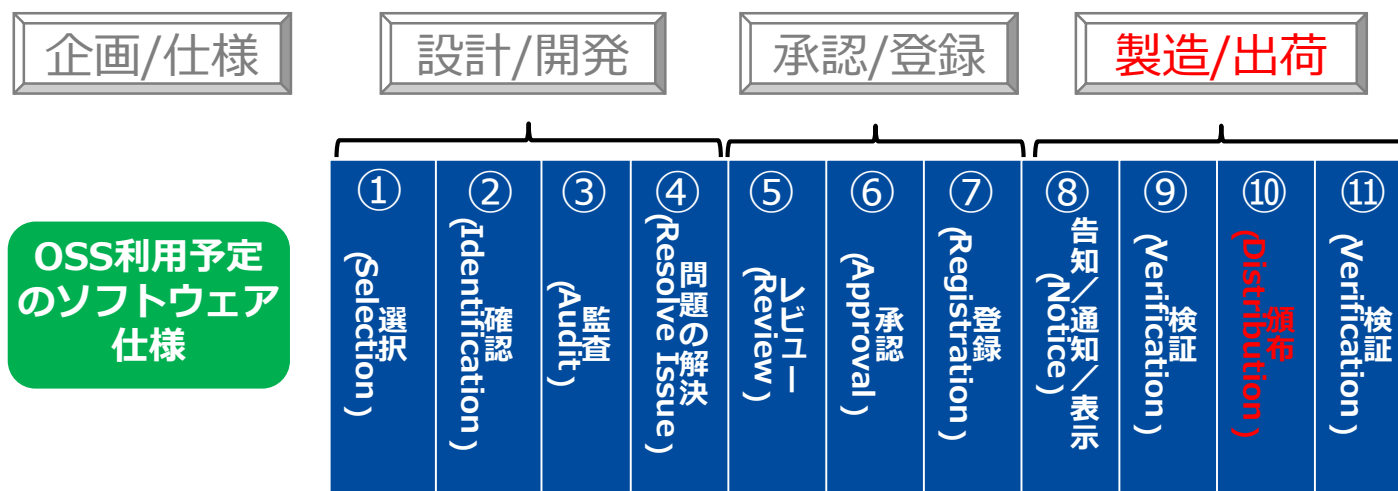
⑩ 頒布

SW360(要検討) :

□ 頒布情報登録

登録例 :

- 公開期間
- 頒布用パッケージ
- ソースコードを公開しているウェブページ



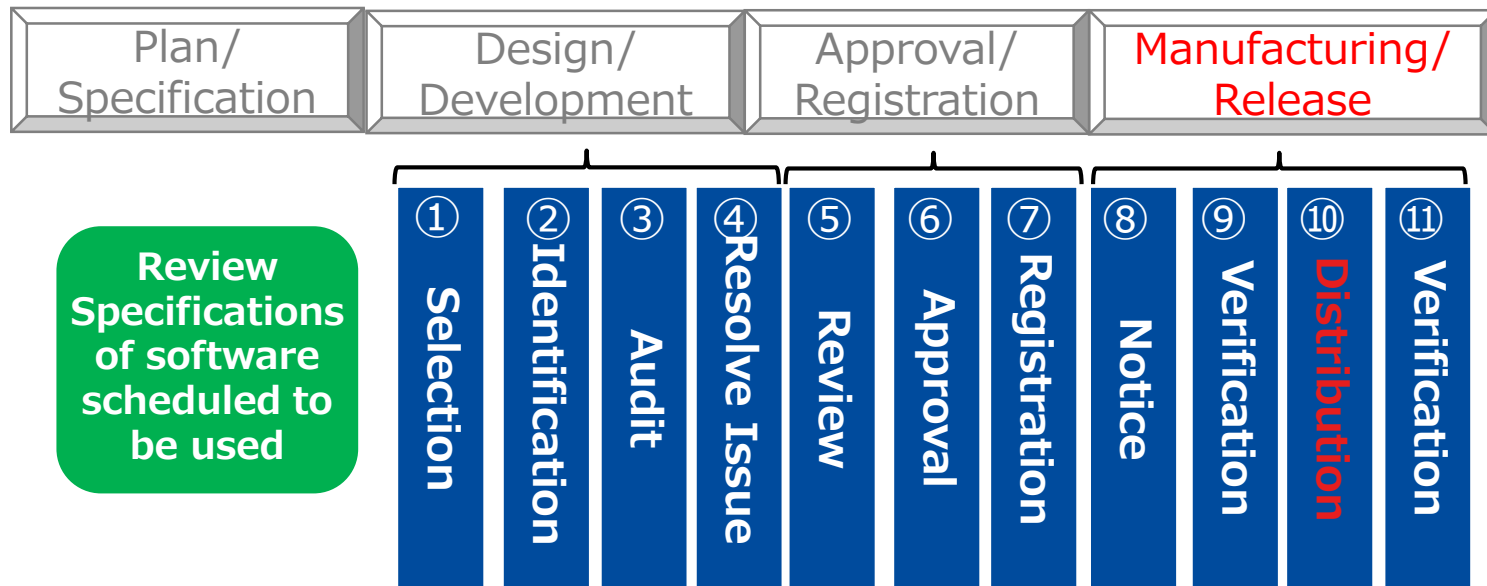
⑩ Distribution

SW360(To be discussed) :

❑ Register `Distribution information`

example :

- Release period
- Package for distribution
- Source code URL



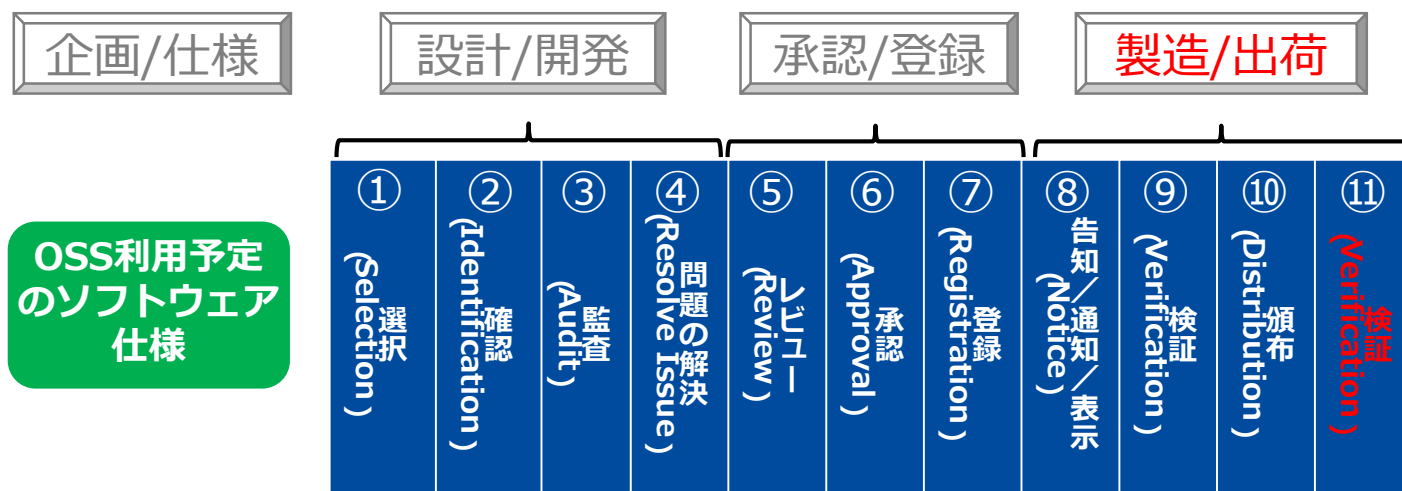
⑪ Verification

SW360 (要検討) :

□ Register the final verification results

やりたいこと

もしウェブ公開する場合は、公開しているサイトから正常にソースコードを入手し、解凍し、製品と同じものが入手でき、コンパイルができることなどを確認



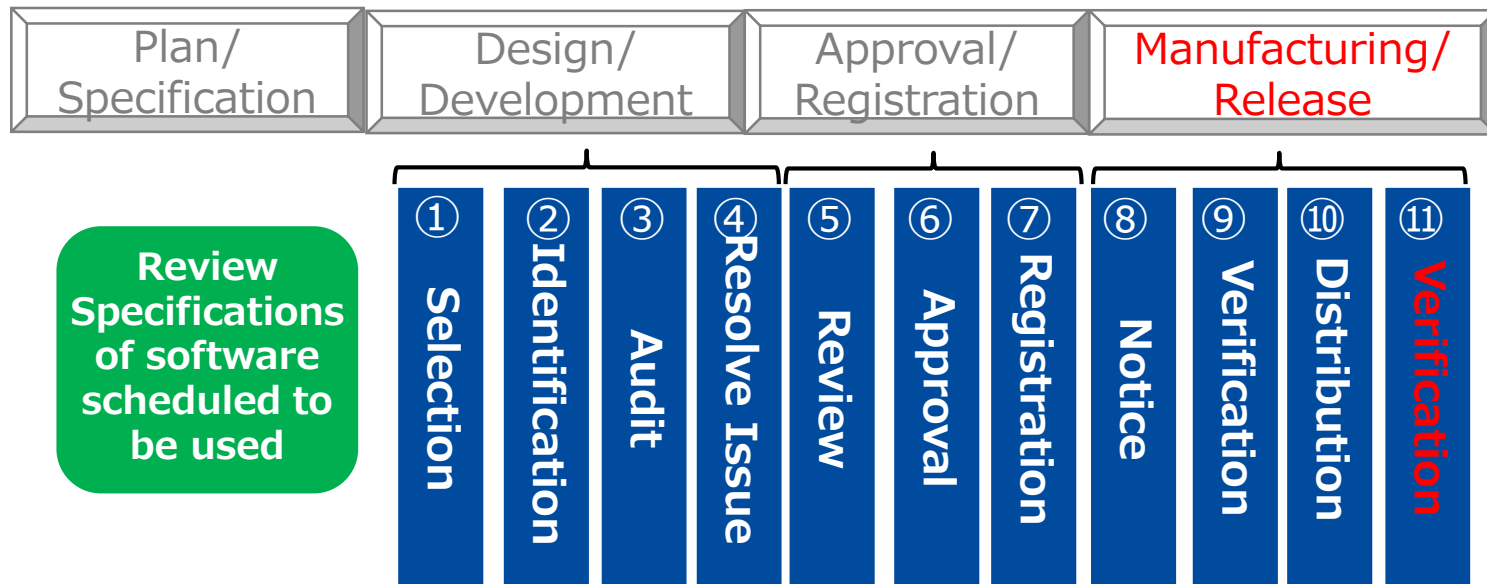
⑪ Verification

SW360 (To be discussed) :

- ❑ Register the final verification results

This step's goal

If you publish it on the web, you can obtain the source code from the published site without any problems, extract it, confirm that you can get the same as the product, and you can compile it.



03

OpenChain Japan WG
Tooling Sub Working Group

SW360についての議論

03

OpenChain Japan WG Tooling Sub Working Group

Discussion
SW360

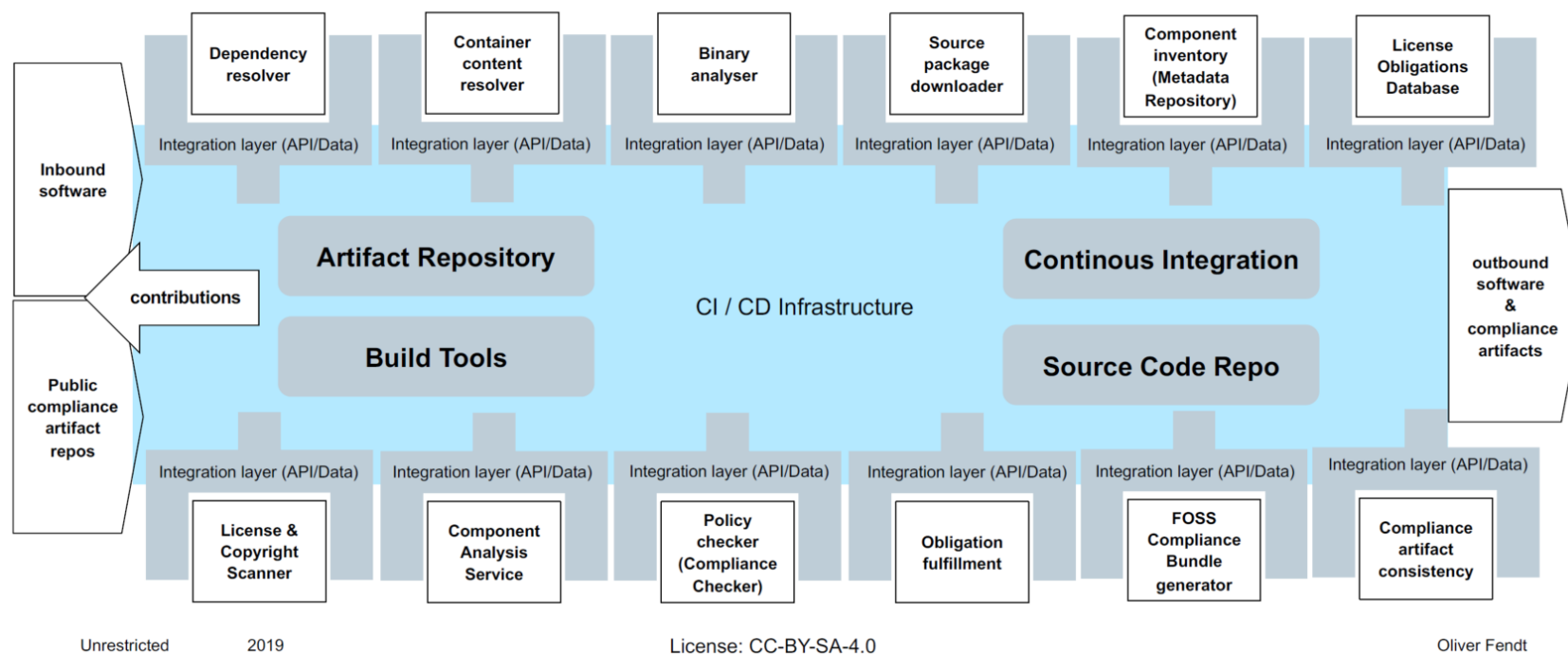
SW360 and OpenChain

OpenChain

Siemens provided SW360 information

- Openchain-japan-wg@lists.linuxfoundation.org
 - Oliver from Siemens has some great slides on the topic. Attached.
 - <https://lists.linuxfoundation.org/mailman/private/openchain-japan-wg/attachments/20190510/f0fd6e60/attachment.pdf>
- https://wiki.linuxfoundation.org/media/openchain/036_oss_to_oling_20190506_fossology_and_sw360_updates_04.pdf

Big Picture – Integrated Compliance Toolchain

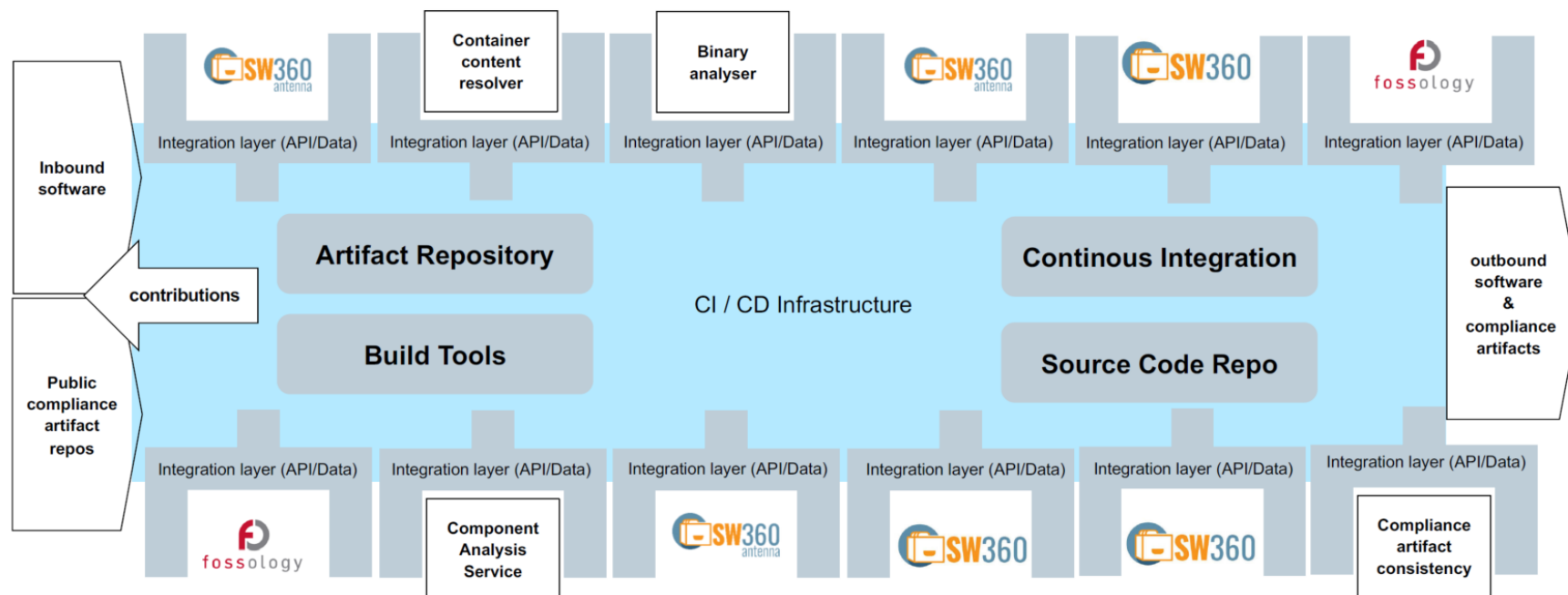


出典([Openchain-japan-wg]メーリングリスト)

<https://lists.linuxfoundation.org/mailman/private/openchain-japan-wg/attachments/20190510/f0fdae60/attachment.pdf>

Big Picture – Integrated Compliance Toolchain Instance

SIEMENS
Ingenuity for Life



Unrestricted

2019

License: CC-BY-SA-4.0

Oliver Fendt

出典([Openchain-japan-wg]メーリングリスト)

<https://lists.linuxfoundation.org/mailman/private/openchain-japan-wg/attachments/20190510/f0fdae60/attachment.pdf>

OpenChain Japan WG Tooling Sub Working Group discussed SW360

OpenChain Japan WG Tooling Sub Working Group

- https://wiki.linuxfoundation.org/openchain/jwg_tooling_sg_page
- <https://wiki.linuxfoundation.org/openchain/minutes>

活動内容（CFPの時点で述べたこと）

- **参加メンバー間でツールに関して議論**
 - 「知りたいこと」
 - 「疑問を持ったこと」
 - 「わかったこと」
 - 「インストール方法や使い方ノウハウ」
 - 「こうなってほしいという希望」
- **F2F を月1回程度、情報共有ツールでは随時、ゆるく議論する**
 - 運営の詳細は参加メンバーで協議
 - F2F開催は単独もしくは他のSWGと共催
 - 情報共有ツールは Slackを想定（メールで適宜補足）
- **成果は、整理してリーダもしくは代行者が Japan WG で報告**

Japan WG Tooling SWGで「やること」

日本語中心でOK

1. ツール情報をまとめる

2. 実際に使いながら勉強や議論をしていく場の提供

- Hands on開催
- ツール紹介開催
- ツール関連のセミナー開催
 - Compass等で案内

3. 情報流通とツールマッピング

4. 活動に賛同するメンバ拡大のためのプロモーション

成果目標の例

- それぞれのツールに関する入手可能な情報をまとめる
- 情報の流通過程とツールのマッピングを行い不足を洗い出す
 - 可能ならば得られた結果を関連するコミュニティへ提案する
- ツールが管理する「データ」そのものの流通手段を検討する
 - SPDXツールやOSS開発コミュニティとの連携方法も含める
- 活動が進んだ時点で、ツール関連のセミナー開催を検討する
 - Open Chain 活動に賛同するメンバ拡大のためのプロモーション

商用ツールの扱いについて

- Antitrust Policyを遵守
 - 特定の商用ツールに対して独占禁止法に抵触する活動は一切しない
 - 推奨や排除など
- 商用ツールに関する活動範囲
 - 特長についての一般的な情報収集
 - 「共通データ」によるベンチマーク結果の取得と比較
 - 異なるデータセットでのベンチマークは行わない
 - 「共通データ」準備については現時点でマイルストーンなし
 - ※商用ツールは一般的な情報の範囲として、アウトプットは外した方が良いというコメントもあり（要検討）

情報収集するツール等の候補（確定ではない）

- コンプライアンス情報取得
 - FOSSology, BlackDuck, FOSSID, BAT (Binary Analysis), Insignary,
 - FOSSology: 動くインストール情報、docker/vagrant 運用
- ライセンス情報 と活用の仕方
 - Github.com/Hitachi/Open-license OSS-license-open data
 - OSADL compliance checklist
- ライセンス情報流通
 - SPDX Tools, SPDX Dashboard, Cleary defined (MS Azure)
- 情報管理
 - Sw360, FOSSA,
 - Sw360詳細検討：バグ情報、動くインストール情報、改変分担、...
- ソースコード管理との連携（カテゴリ分けが変かも）
 - GitLab, Yocto,
- 使用状況、ユースケース、リスト化
 - doubleOpen(?), BlackDuck Hub
- **Double Open Landscape Survey**

This slide is
only Japanese
Language



<https://github.com/doubleopen-project/doubleopen-publications/blob/master/publication.md#double-open-landscape-survey>

Open Chain Japan Tooling Group で SW360議論

ツールの設定方法が複雑で動作が不安定な問題

- インストール時
 - インストールがうまくいった環境やSW360のバージョンをシェアしあう
 - あらかじめ作戦で決めたパターンを試して成否の記録を残し、整理する
 - Dockerでインストールできない例
 - <https://github.com/sw360/sw360chores/issues/52>
 - Vagrantの例
 - <https://github.com/sw360/sw360vagrant/issues/9>
- 動作時
 - 初期設定方法が不明瞭
 - 設定例設定方法共有
 - 実行中に確認した不可解な動作を共有
 - バグか仕様か確認
 - Github上にissue報告
 - 他ツールとの連携情報共有
 - 既にある特定のツールと連携方法共有
 - <https://github.com/sw360/sw360bdpImportService>

Open Chain Japan Tooling Group で SW360議論

ツールの設定方法が複雑で動作が不安定な問題

- インストール時
 - インストールがうまくいった環境やSW360のバージョンをシェアしあう
 - あらかじめ作戦で決めたパターンを試して成否の記録を残し、整理する
 - Dockerでインストールできない例
 - <https://github.com/sw360/sw360chores/issues/52>
 - Vagrantの例
 - <https://github.com/sw360/sw360vagrant/issues/9>
- 動作時
 - 初期設定方法が不明瞭
 - 設定例設定方法共有
 - 実行中に確認した不可解な動作を共有
 - バグか仕様か確認
 - Github上にissue報告
 - 他ツールとの連携情報共有
 - 既にある特定のツールと連携方法共有
 - <https://github.com/sw360/sw360bdpImportService>

Open Chain Japan Tooling Group で SW360議論

* パフォーマンスが運用ルールに依存 *

- 運用ルールを決めないと、想定したパフォーマンスがでない可能性がある。
- パッケージの依存関係が分かるように登録するにはどうすればいいか？アイデア共有。
- 登録命名規則
- (日本のソフトウェア開発事情に即した?)運用しやすいコンポーネントやプロジェクト名の命名規則は何か？
- 脆弱性情報取得効率化とCPE IDの利用方法
- cvesearch.default.*.threshold のおすすめパラメータ
- <https://github.com/eclipse/sw360/wiki/User-Vulnerability-Management>
- CPE IDで表記しにくいコンポーネントもあり、その対処方法を共有

Open Chain Japan Tooling Group で SW360議論

* パフォーマンスが運用ルールに依存 *

- 運用ルールを決めないと、想定したパフォーマンスがでない可能性がある。
- パッケージの依存関係が分かるように登録するにはどうすればいいか？アイデア共有。
- 登録命名規則
- (日本のソフトウェア開発事情に即した?)運用しやすいコンポーネントやプロジェクト名の命名規則は何か？
- 脆弱性情報取得効率化とCPE IDの利用方法
- cvesearch.default.*.threshold のおすすめパラメータ
- <https://github.com/eclipse/sw360/wiki/User-Vulnerability-Management>
- CPE IDで表記しにくいコンポーネントもあり、その対処方法を共有

Open Chain Japan Tooling Group discussed SW360

"Settings are complex, and tool operation is unstable "

* Issue: (Installation)

sw360 depends on many OSS components (and their versions) and needs many settings. When we install sw360, it is difficult to find correctly working combination of component versions and settings. If combination is in correct, the tool does not work at all. In addition, updates of OSS components may turn correct combination into incorrect combination.

AI:

To search systematically the correct combination to work and record the results. (e.g. combination of Linux distribution and sw360chores)
To share the result in the subgroup.

Examples:

Failure in Docker installation

<https://github.com/sw360/sw360chores/issues/52>

Failure in Vagrant installation

<https://github.com/sw360/sw360vagrant/issues/9>

* Issue: (Operation)

Initial settings are not clear.

AI:

To share settings in the subgroup.

* Issue: (Operation)

Unexpected behaviors

AI:

To share unexpected behaviors.

To verify if it is specification or bug.

To report it in ISSUE of GitHub.

To share reference configuration.

* Issue: (Operation)

Importing service is unknown by many people.

AI:

To share information in the subgroup.

Example:

<https://github.com/sw360/sw360bdpImportService>

Open Chain Japan Tooling Group discussed SW360

"Need effective standardized operation rules"

*Issue:

Operation rule may affect sw360 performance. But users do not know how to define appropriate operation rule.

AI:

To share idea.

How to define dependency of packages in sw360.

* Issue:

Component naming rule affects accuracy of getting vulnerability information.

AI:

How to define naming rule of components. Naming rule should be considered in the way that Japanese engineers can operate easily.

* Issue:

Relation between getting vulnerability information and CPE ID

There is recommended parameters for cvesearch.default.*.threshold

<https://github.com/eclipse/sw360/wiki/User-Vulnerability-Management>

It is difficult to learn CPE ID.

Some components are difficult to be described by CPE ID.

AI:

To discuss idea.

"Localization"

*Issue:

Current ECC (Export Control Classification) support page is not applicable to Japan.

<https://github.com/eclipse/sw360/issues/406>

AI:

To describe how companies use ECC in Japan.

To share idea to modify ECC in the subgroup.

04

まとめ



- SW360
 - どんな機能があればいいか今後も議論したい
 - どのように運用するかを含めて今後議論したい
 - OpenChainJapan Tooling Sub Groupでも議論中
- It is good to discuss the required function
- It is good to discuss the way to operate SW360
- OpenChainJapan Tooling Sub Group discusses SW360

Open Source Summit Japan 7月18日 (木)
16:50-17:30

Using SW360 for OSS Compliance Management
Process - Kouki Hama , Toshiba

<https://ossalsjp19.sched.com/event/OVtF/using-sw360-for-oss-compliance-management-process-kouki-hama-toshiba>

ご参加 & フィードバックお願いいたします！
Please join !

TOSHIBA

ご清聴ありがとうございました